

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY**

THE HOMESOURCE, CORP. Plaintiff, vs. RETAILER WEB SERVICES, LLC and JOHN DOES 1-3, Defendants.	Case No. 1:18-cv-11970 (JBS-KMW) DECLARATION OF KEVIN TUTEN
---	---

I, Kevin Tuten, declare under the penalty of perjury as follows:

1. I was engaged by the plaintiff The HomeSource Corp. (“HomeSource”) in connection with the above-captioned matter. I have personal knowledge of the facts stated herein and these facts are true to the best of my knowledge, information and belief.

2. I spent many hours working with the defendant RWS’s expert, Dr. Bayuk, attempting to agree on a protocol for searching HomeSource’s logs for RWS’s IP addresses. I understood that these were my instructions and we worked hard to try to reach agreement. I was instructed to attempt to agree on a protocol that assumed that RWS’s list of IP addresses would be designated “Attorneys Eyes Only,” and therefore, not given to HomeSource. However, the designation of RWS’s IP addresses as “Attorneys Eyes Only” inserted a lot of difficulty and confusion into the process.

3. First, I never understood the basis for treating RWS’s IP addresses as highly confidential. These same IP addresses are in the hands of numerous third parties. Every time RWS visits a website, it gives the owner of that website its IP address. RWS’s IP addresses are assigned to RWS by a third party, and if RWS visited HomeSource’s websites, the IP addresses

are already in the possession of HomeSource. I am not aware of any basis to designate the IP addresses “confidential” or “Attorneys Eyes Only” and no basis for the designation was ever explained to me.

4. Second, the vision of how this search would go appeared to be that Dr. Bayuk and I would (1) take HomeSource’s logs; (2) take RWS’s IP addresses; and (3) compare them and produce a report on our own, without the participation of HomeSource. This was never possible for the reason that “HomeSource’s logs” consist of a massive amount of data in binary format, which is only understood and interpreted through software that was customized by HomeSource. This is not similar to two experts analyzing comparing files in a standard software program, such as “Microsoft Word.” HomeSource has built a unique system on its own, and as outsiders, we the experts were never going to be able to understand that system without additional information and guidance from HomeSource.

5. Despite these two hurdles, we attempted to reach agreement. This resulted in Dr. Bayuk and RWS’s attorneys asking to speak with HomeSource employees as part of the process, so that they could understand HomeSource’s unique system, and numerous questions being directed to HomeSource by the experts and RWS’s attorneys through HomeSource’s counsel. Ultimately, we thought we had reached an agreed protocol. We presented HomeSource with the protocol and discovered that this protocol essentially would not work as we had envisioned.

6. Dr. Bayuk acknowledges this difficulty when she states in her January 21, 2019 summary, that our final proposal was that: “These steps included having a HS staff member physically located near me to teach us how to use the search tool and to show us search results that HS had collected from prior searches (but not participate in the actual search for the RWS’s IP

addresses).” Dr. Bayuk is correct that HomeSource would need to teach both of us to use the search tool and assist us in understanding the search results, by providing additional information.

7. In sum, our need for a large amount of information from HomeSource, in exchange for a simple list of IP addresses from RWS, was always in conflict with our “marching orders,” which were that we were to keep the IP addresses “Attorneys Eyes Only” and exclude HomeSource from the process.

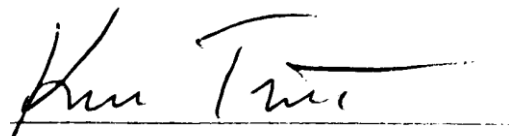
8. My understanding is that after our attempts to reach agreement broke down, HomeSource obtained IP addresses associated with RWS from third parties, ran searches for those IP addresses, and produced the search results to RWS. This was a much simpler way of conducting the search.

9. Throughout all of our discussions, another assumption was that a complete list of IP addresses would be provided by RWS. RWS’s final draft protocols contained the statement that “all IP addresses utilized by RWS employees, principals and agents” would be provided by RWS. RWS also agreed to the following statement, which was in all the drafts: “This protocol assumes that RWS did not utilize a VPN or “masked” IPs, per RWS’s counsel’s email of December 5, 2018.” RWS removed its agreement to provide all IP addresses utilized by RWS employees, principals and agents and that is when the discussions broke down.

10. Unless we have a complete list of RWS’s IP addresses, then we will never be able to determine the extent of RWS’s activity in HomeSource’s logs.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on March 8, 2019

A handwritten signature in black ink, appearing to read "Kim T. [unclear]", written over a horizontal line.